IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: William J. Beyda	Art Unit	: 2152
Serial No.	: 09/668,039	Examiner	: Refai, Ramsey
Filed	: September 21, 2000	Confirmation No.: 9089	
Title	: PROCESSING ELECTRONIC MESSAGES		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

I. Introduction

Claims 1-5, 14-18, and 29-38, which are the subject of this appeal, are pending.

The Examiner has rejected claims 1-5, 14-18, and 29-38 as follows:

- Claims 1-5, 14-18, and 29-38 stand rejected under 35 U.S.C. § 103(a) over Fields (U.S. 6,704,797) in view of Sato (U.S. 6,914,691).

II. The Examiner's response to the Appeal Brief and Appellant's rebuttal

1. Independent claim 1

a. Introduction

The rejection of claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato should be withdrawn because (i) the Examiner has not established a *prima facie* case of obviousness, and (ii) one skilled in the art would not have had any apparent reason to combine the references in the manner proposed by the Examiner.

CERTIFICATE OF TRANSMISSION

I hereby certify that this document is being transmitted to the Patent and Trademark Office via electronic filing

July 25, 2008
Date of Transmission

(Signature of person mailing papers)

Edouard Garcia
(Typed or printed name of person mailing papers)

b. The Examiner's Answer A

The Examiner has taken the position that the client web browser request disclosed in Fields constitutes an electronic message in which the access manager 34 "is configured to detect an access restriction notice," as recited in claim 1 (see, e.g., page 2, § 4, second ¶ of the Office action dated September 1, 2006; also see page 3, § 3, second ¶ of the Supplemental Answer). In the Appeal Brief, appellant explained that none of the client-specific data in a given client request constitutes an "access restriction notice" within the plain meaning of the term (see § VII.A.4.c.i of the Amended Appeal Brief). In response, the Examiner has stated without explanation that the "broadest reasonable interpretation" of "access restriction notice" encompasses the client-specific data contained in the client web browser request (see page 6, Argument A of the Supplemental Answer).

On its face, the term "access restriction notice" refers to a notice of restricted access. This interpretation is confirmed by the plain meanings of the constituent words "access", "restriction", and "notice". In the context of the subject matter defined in claim 1, the plain meaning of the term "access" is a "freedom or ability to obtain or make use of" (definition 2b in Merriam-Webster's Collegiate Dictionary, Tenth Edition, 1995); the plain meaning of the term "restriction" is "a limitation on the use or enjoyment of property or a facility" (definition 1b in Merriam-Webster's Collegiate Dictionary, Tenth Edition, 1995); and the plain meaning of the term "notice" is a "warning or intimation of something: ANNOUNCEMENT" (definition 2b in Merriam-Webster's Collegiate Dictionary, Tenth Edition, 1995). Thus, in accordance with the plain meanings of its constituent words, the term "access restriction notice" means a warning or announcement of a limitation on the freedom or ability to obtain or make use of.

The only client-specific data explicitly disclosed in Fields is as follows: "an identity of a referring page (i.e. the page from which the link to the server was selected), a client machine IP address, the identity of a third party service provider (e.g., an ISP) that provides Internet service to the client, the existence (or lack thereof) of a user authentication, a user identifier such as a cookie, or other such data" (col. 4, lines 25-32). The identifier and address information that makes up the client-specific data disclosed in Fields does not provide any notice, warning, or announcement of restricted access or limitation on the freedom or ability to obtain or make use

of anything. Thus, the client-specific data disclosed in Fields does not constitute an "access restriction notice."

The Examiner has not provided any basis for believing that the "broadest reasonable interpretation" of "access restriction notice" is inconsistent with the plain meaning of the term; indeed, the Examiner has not explained in any way how he has interpreted the term "access restriction notice". Therefore, there is no reasonable basis for the Examiner's assertion that the plain meaning of the term "access restriction notice" encompasses any of the types of client-specific data disclosed in Fields.

For the reasons explained above, Fields in view of Sato does not disclose or suggest the access restriction notice defined in claim 1. Since the cited references do not disclose or suggest each and every one of the elements of claim 1, the rejection of claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato must be withdrawn.

c. The Examiner's Answer B

In § VII.A.4.c.i of the Amended Appeal Brief, appellant explained that since Fields does not disclose or suggest an "access restriction notice" as defined in claim 1, Fields cannot possibly disclose or suggest an access restriction filter that is configured to detect an access restriction notice in the respective ones of the electronic messages, as recited in claim 1. In response to this point, the Examiner simply repeated his belief that the client-specified data disclosed in Fields constitutes an access restriction notice (see page 7, Argument B of the Supplemental Answer). For the reasons explained in the preceding section, however, Fields does not in fact disclose an "access restriction notice" and consequently Fields' access manager 34 does not constitute an access restriction filter as defined in claim 1.

In § VII.A.4.c.i of the Amended Appeal Brief, appellant also explained that Sato does not make-up for the failure of Fields to disclose or suggest an "access restriction filter is configured to detect an access restriction notice in the respective ones of the electronic messages," as recited in claim 1. The Examiner has not expressed any disagreement with this point.

For the reasons explained above, Fields in view of Sato does not disclose or suggest the access restriction filter defined in claim 1. Since the cited references do not disclose or suggest

each and every one of the elements of claim 1, the rejection of claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato must be withdrawn.

d. The Examiner's Answer C

In § VII.A.4.c.ii of the Amended Appeal Brief, appellant explained that one skilled in the art at the time the invention was made would not have been led to combine the teachings of Fields and Sato to arrive at the inventive electronic messaging system recited in claim 1. For example, Sato's copyright-information detecting circuit 105 operates on raster image data that is produced by the print controller 102 (see col. 8, lines 1 - 34, and col. 7, lines 35-45), but Field's client-specific data (which the Examiner has assumed to be an access restriction notice) does not contain any raster image data that could be processed by Sato's copyright-information detecting circuit 105.

Appellant pointed out that the Examiner has not explained how Sato's detecting circuit 105, which is designed to apply pattern matching or character recognition techniques to raster image data, could be applied to web browser requests that do not contain such raster image data. Clearly, it is not possible to say that it would have been obvious to one skilled in the art to combine the teachings of Fields and Sato without specifying the details of that proposed combination. In effect, without specifying the details of the proposed combination of the reference teachings that is envisioned by the Examiner, the Examiner's basis for rejecting claim 1 amounts to no more than an impermissible conclusory statement that cannot support a rejection under 35 U.S.C. § 103. In fact, the inability of the Examiner to articulate the details of his proposed combination evidences the unobviousness of the Examiner's proposed combination.

Inexplicably, the Examiner did not respond to either of these points in his Answer (see Argument C on pages 8-9 of the Supplemental Answer). Instead, the Examiner argued that (Supplemental Answer, page 8, sixth line from bottom - page 9, line 2):

> ...Sato teach a detection process for detecting copyright restriction characters on images and executes pattern matching with characters stored in memory to impose stored restriction policies, such as prevent copying of the image (column 8, lines 9-34). It would have been obvious to one of the ordinary skill in the art to combine the teachings of Fields et al and Sato because doing so

> would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image. The claims recite combinations which only unite elements with no change in their respective functions and which yield predictable results. Thus the claimed subject matter likely would have been obvious under *KSR*.

This argument, however, does not explain how one skilled in the art would have been led to operate Sato's image-based copyright-information detecting circuit 105 on the non-image-based identifiers and addresses that constitute the client-specific data disclosed in Fields. Without such an explanation, the Examiner's rationale amounts to no more than a conclusory statement that cannot support a rejection under 35 U.S.C. § 103. See KSR Int'l Co. v. Teleflex Inc., No. 127 S. Ct. 1727, 1741 (2007) (citing In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006): "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."

In § VII.A.4.c.ii of the Amended Appeal Brief, appellant also explained that one skilled in the art at the time the invention was made would not have been motivated to combine the teachings of Fields and Sato in the manner proposed by the Examiner because such a combination would not serve any useful purpose whatsoever. For example, the client requests for images or web pages containing images do not contain the images whose access is being controlled by Fields' access manager 34 - indeed, these client requests would not be made if they already contained the images. Therefore, one skilled in the art would not have any reason whatsoever to use Sato's detection circuit 105 to detect the presence of a copyright indication in the client requests that are received by Fields' access manager 34. Inexplicably, the Examiner did not respond to this point in his Answer.

In § VII.A.4.c.ii of the Amended Appeal Brief, appellant also explained that the motivation (i.e., "because doing so would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image") cited in support of his proposed combination of Fields and Sato would not have given one skilled in the art any apparent reason to combine the reference teachings in the manner proposed by the Examiner. In particular, the possibility that the combined teaching "would

create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image" does not constitute a showing of a suggestion or a motivation, either in the cited references themselves or in the knowledge generally available, that would have given one skilled in the art any apparent reason to modify the references or to combine the reference teachings, especially in light of the fact that the client requests handled by Fields' access manager 34 do not include any raster image data, much less do they contain the images whose access is being controlled by Fields' access manager 34. Inexplicably, the Examiner did not respond to this point in his Answer.

In addition, appellant explained that there is no basis whatsoever for the Examiner's conclusion that a combination of Fields and Sato "would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image." In this regard, appellant asked the Examiner to explain how the detection of copyright-information in non-existent image data in client web browser requests "would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image" when the client web browser requests do not contain the protected images (see § VII.A.4.c.ii of the Amended Appeal Brief). Inexplicably, the Examiner did not respond to this point in his Answer.

Instead of pointing to some teaching or suggestion in Fields, or Sato, or the knowledge generally available to support the proposed combination of Fields and Sato, the Examiner has relied on circular reasoning. In particular, the Examiner's proffered motivation (i.e., "because doing so would create a way to detect copyright symbols on protected images and determine what restriction needs to be imposed on distribution of the protected image") assumes the result (i.e., the modification of Fields' system) to which the proffered "motivation" was supposed to have led one skilled in the art. Such circular reasoning cannot possibly support a rejection under 35 U.S.C. § 103(a). Indeed, such circular reasoning only evidences the fact that the Examiner improperly has engaged in impermissible hindsight reconstruction of the claimed invention, using applicants' disclosure as a blueprint for piecing together elements from the prior art in a manner that attempts to reconstruct the invention recited in claim 1 only with the benefit of impermissible hindsight (see KSR at 1744: "A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon ex post

reasoning."). The fact is that neither Fields nor Sato nor the knowledge generally available at the time the invention was made would have led one skilled in the art to believe that there was any problem to be solved or any advantage that would be gained by the Examiner's proposed modification of Fields' system.

Without any apparent reason for modifying Fields' disclosure, the Examiner's rationale in support of the rejection of claim 1 amounts to no more than a conclusory statement which cannot support a rejection under 35 U.S.C. § 103. See KSR at 1741 (citing In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006): "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

For at least this additional reason, the rejection of claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato should be withdrawn.

e. Conclusion

As explained in detail above, the rejection of claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato should be withdrawn because (i) the Examiner has not established a *prima facie* case of obviousness, and (ii) one skilled in the art would not have had any apparent reason to combine the references in the manner proposed by the Examiner.

For these reasons and the reasons given in the Appeal Brief, the rejection of independent claim 1 under 35 U.S.C. § 103(a) over Fields in view of Sato should be withdrawn.

2. Dependent claims 2-5, 30, and 33-35

Each of claims 2-5, 30, and 33-35 incorporates the features of independent claim 1 and therefore is patentable over Fields in view of Sato for at least the same reasons explained above and in the Appeal Brief.

The Examiner's rejections of claims 2-5 and 33 also should be withdrawn for the following additional reasons.

a. Claim 2 - Examiner's Answer D

In § VII.A.5.a, appellant explained that Fields' disclosure does not support the Examiner's contention that Fields teaches that "the access restriction filter is configured to detect in respective ones of the electronic messages an access restriction notice indicating ownership of at least a portion of the respective ones of the electronic message," as recited in claim 2.

The Examiner responded to this point as follows (page 9, Argument D of the Supplemental Answer):

> In response, the Examiner respectfully disagrees. The detecting of images that contain watermark or company logos indicates ownership of an image (column 2, lines 51-53, column 5, lines 40-67).

In § VII.A.5.a, appellant explained that the watermark or company logos discloses in col. 2, lines 51-53, and col. 5, lines 40-67, are not contained in the client web browser requests; instead, they are contained on the server. In particular, the cited sections of Fields disclose an example of a policy rule that restricts distribution of a protected to a modified version of the image that is overlaid with a company logo or watermark. This disclosure relates to the type of image that is served in response to the client web browser request. This disclosure does not change the fact that the access manager 34 evaluates client-specific data in the request against client-specific access criteria specified in the policy rule; the access manager 34 does not detect anything whatsoever in the protected images or the image versions derived from the protected images. Inexplicably, the Examiner did not respond to this point in his Answer.

b. Claim 3 - Examiner's Answer E

In § VII.A.5.b, appellant explained that Fields' disclosure does not support the Examiner's contention that Fields teaches that "the access restriction filter is configured to detect a copyright notice in respective ones of the electronic messages," as recited in claim 3.

The Examiner responded to this point as follows (page 9, Argument E of the Supplemental Answer):

> In response, the Examiner respectfully disagrees. Fields teaches a method to protect images via a server-based policy (see at least column 2, lines 37-38). When a client requests and image or a web page containing the image, the method parses the request and examines the image. A rule for the image is evaluated against client specific data. If the condition is satisfied an image restriction is imposed. (See at least column 1, lines 35-67, column 2, line 36- column 3, line 15, column 7, lines 40-67).

On its face, the Examiner's response does not show that Fields discloses an access restriction filter that is configured to detect a copyright notice in respective ones of the electronic messages. Instead, this response merely shows that Fields' method evaluates a rule for an image on a server against client-specific data contained in a client web browser request.

In addition, the cited sections of Fields do not support the Examiner's position.

- Col. 2, lines 37-38, discloses that digital content may be transmitted and distributed to many users over the world wide web. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect a copyright notice in respective ones of the electronic messages.
- Col. 1, lines 35-67, discloses that in an open system copyrighted content may be transmitted and distributed freely to many users over the world wide web. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect a copyright notice in respective ones of the electronic messages.
- Col. 2, line 36 - col. 3, line 15, discloses that Fields' invention evaluates a rule for an image on a server against client-specific data contained in a client web browser request. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect a copyright notice in respective ones of the electronic messages.
- Col. 7, lines 40-67, discloses the advantages and uses of Fields' system. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect a copyright notice in respective ones of the electronic messages.

c. Claim 4 - Examiner's Answer F

In § VII.A.5.c, appellant explained that Fields' disclosure does not support the Examiner's contention that Fields teaches that "the access restriction filter is configured to detect the copyright notice by comparing one or more characters in the respective ones of the electronic

messages to respective characters of one or more copyright notices stored in memory," as recited in claim 4.

The Examiner responded to this point as follows (page 9, Argument F of the Supplemental Answer):

> In response, the Examiner respectfully disagrees. Fields teaches a method to protect images via a server-based policy (see at least column 2, lines 37-38). When a client requests and image or a web page containing the image, the method parses the request and examines the image. This data is then compared to the distribution criteria in the rule (see at least column 3, lines 11-12, column 5, lines 27-30).

On its face, the Examiner's response does not show that Fields discloses an access restriction filter that is configured to detect the copyright notice by comparing one or more characters in the respective ones of the electronic messages to respective characters of one or more copyright notices stored in memory. Instead, this response merely shows that Fields' method evaluates a rule for an image on a server against client-specific data contained in a client web browser request.

In addition, the cited sections of Fields do not support the Examiner's position.

- Col. 2, lines 37-38, discloses that digital content may be transmitted and distributed to many users over the world wide web. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect the copyright notice by comparing one or more characters in the respective ones of the electronic messages to respective characters of one or more copyright notices stored in memory.
- Col. 3, lines 11-12, discloses that Fields' method parses the request to identify specific data pertaining to the requesting client. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect the copyright notice by comparing one or more characters in the respective ones of the electronic messages to respective characters of one or more copyright notices stored in memory.
- Col. 5, lines 27-30, discloses that the access manager compares client-specific data associated with a given client request to the rules criteria of a given policy and selects the image version to serve. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect the copyright notice by comparing one or more characters in the respective ones of the electronic

> messages to respective characters of one or more copyright notices stored in memory.

d. Claim 5 - Examiner's Answer F (repeated)

In § VII.A.5.d, appellant explained that Fields' disclosure does not support the Examiner's contention that Fields teaches that "the access restriction filter is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices," as recited in claim 5.

The Examiner responded to this point as follows (page 10, Argument F (repeated) of the Supplemental Answer):

> In response, the Examiner respectfully disagrees. Fields et al teach that a client specific data can include a client machine IP address, image URL, and user authentication which are all known to be stored in the header component of an electronic message (see at least column 4, lines 25-33, column 6, lines 1-10, column 5, lines 57-60). Also, Fields teach that a server that implements the image protection scheme can examine the header of an image request to determine appropriate action (column 5, lines 1-5).

On its face, the Examiner's response does not show that Fields discloses an access restriction filter that is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices. Instead, this response merely argues that Fields' client-specific data might be contained in "header component" of a client web browser request. This argument, however, does not show that Fields' access manager 34 is configured to detect a copyright notice by comparing characters in a header component of the client web browser request with respective characters of the one or more stored copyright notices.

In addition, the cited sections of Fields do not support the Examiner's position.

- Col. 4, lines 25-33, discloses that representative client-specific data include: an identity of a referring page (i.e. the page from which the link to the server was selected), a client machine IP address, the identity of a third party service provider (e.g., an ISP) that provides Internet service to the client, the existence (or lack

thereof) of a user authentication, a user identifier such as a cookie, or other such data; and that these examples of client-specific data are merely exemplary. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices.

- Col. 6, lines 1-10, discloses that when a request for the image is received, the image distribution manager determines whether the requested URL has an associated distribution policy. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices.
- Col. 5, lines 57-60, discloses that a given image version may be associated with any requests that originate from a given IP address, a given user group, or the like. This section of Fields does not disclose or suggest an access restriction filter that is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices.
- Col. 5, lines 1-5, discloses that Fields' system examines "Referer" headers whenever an image request is received, where the "Referer" header " specifies the URL of the document from which the link was followed (see col. 4, lines 53-67). This section of Fields does not disclose or suggest an access restriction filter that is configured to detect the copyright notice by comparing characters in a header component of the respective ones of the electronic messages with respective characters of the one or more stored copyright notices.

e. Claim 33 - Examiner's Answer G

In § VII.A.5.e, appellant explained that Fields' disclosure does not support the Examiner's contention that Fields teaches that "at least one of the electronic messages comprises a primary message and at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices," as recited in claim 33.

The Examiner responded to this point as follows (page 10, Argument G of the Supplemental Answer):

> In response, the Examiner respectfully disagrees. Fields et al teach that the server performs the restriction policy on requested web

pages that include images (column 6, lines 1-4, column 5, lines 40-41, column 4, lines 34-39).

On its face, the Examiner's response does not show that Fields discloses that at least one of the electronic messages comprises a primary message and at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices. Instead, this response merely argues that Fields' server performs the restriction policy on requested web pages that include images. This argument, however, does not show that Fields discloses anything whatsoever relating to an attachment to the client web browser request (which the Examiner asserts as the electronic message recited in claim 1).

In addition, the cited sections of Fields do not support the Examiner's position.

- Col. 6, lines 1-4, discloses that when a request for the image is received, the image distribution manager determines whether the requested URL has an associated distribution policy. This section of Fields does not disclose or suggest that at least one of the electronic messages comprises a primary message and at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices.
- Col. 5, lines 40-41, discloses that the image is located at a specified URL at the web server. This section of Fields does not disclose or suggest that at least one of the electronic messages comprises a primary message and at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices.
- Col. 4, lines 34-39, discloses that a set of image versions are stored at the server; a given image version may then be associated with given client-specific data; and when a given client request for the image (or for a page that includes the image) is received at the server, the image version whose associated distribution criteria matches (or, alternatively, best matches) the client-specific data is then served. This section of Fields does not disclose or suggest that at least one of the electronic messages comprises a primary message and at least one attachment, and the access restriction filter is configured to compare characters in the primary message and characters in the at least one attachment to respective characters of the one or more stored access restriction notices.

III. Conclusion

For the reasons explained above, all of the pending claims are now in condition for allowance and should be allowed.

Charge any excess fees or apply any credits to Deposit Account No. 19-2179.

Respectfully submitted,

Date: July 25, 2008

Edouard Garcia
Reg. No. 38,461
Telephone No.: (650) 965-8342

Please direct all correspondence to:

SIEMENS CORPORATION
Intellectual Property Department
170 Wood Avenue South
Iselin, New Jersey 08830
ATTENTION: Elsa Keller, IP Department
Telephone: (732) 321-3026